Printed in U.S.A.
Vol. 110, No. 2

Online Essay

THE CURIOUS CASE OF CELL PHONE LOCATION DATA: FOURTH AMENDMENT DOCTRINE MASH-UP[†]

Monu Bedi

ABSTRACT—Police surveillance ability and information gathering capacity have a dynamic relationship with technology. Greater advancements in technology make it easier for the police to surveil individuals and collect information. This state of affairs leads to heightened concerns over Fourth Amendment protection. This issue has most recently played out in the context of police collecting cell phone location data. Courts disagree on whether and to what extent this data garners Fourth Amendment protection. Underlying this disagreement rests a hitherto overlooked tension between two interrelated Fourth Amendment doctrines—the third-party and the public disclosure doctrines. While both vitiate privacy protection and are commonly associated together, they rely on very different triggers. This Essay provides a detailed analysis of these distinct features in an effort to harmonize the doctrines in the cell phone location data context.

AUTHOR—Associate Professor of Law, DePaul University College of Law, A.B. Dartmouth, M.Phil. Cambridge, J.D. Harvard. I would like to thank the editors of the *Northwestern University Law Review Online*, and specifically William Gohl and Carlo Felizardo, for their excellent editing work.

[†] This Essay was originally published in the *Northwestern University Law Review Online* on October 29, 2015, 110 NW. U. L. REV. ONLINE 61 (2015), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1227&context=nulr_online [http://perma.cc/SX4B-33KG].

INTRODUCTION

The third-party and public disclosure doctrines are longstanding hurdles to Fourth Amendment protection. Federal courts have recently invoked these doctrines to determine whether police can acquire cell phone location data from providers without constitutional scrutiny.[1] These rulings are all over the map. Courts disagree not only on whether location information is constitutionally protected but also if one, both, or neither of these doctrines applies. The Supreme Court has yet to enter the fray. So for now, we are left with muddled results.[2] A major reason for the confusion turns out to rest on a hitherto overlooked tension between the two doctrines. This Essay is the first to raise this issue and, in turn, harmonize these doctrines in the cell phone location data context.[3]

While both doctrines vitiate privacy protection and are often associated together, they rest on unique foundational triggers.[4] The third-party doctrine involves an individual voluntarily disclosing nonpublic

[1] *See infra* Part III.

[2] *See, e.g.*, Orin Kerr, *When and How Will the Supreme Court Enter the Cell-Site Fray?* WASH. POST: THE VOLOKH CONSPIRACY (Aug. 5, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/05/when-and-how-will-the-supreme-court-enter-the-cell-site-fray [http://perma.cc/U6YR-VR6Z].

[3] This Essay focuses exclusively on constitutional protection without reference to statutory authority or any good faith exception analysis. For an example of such analysis, see generally *id.*

[4] *See infra* Sections II.A–B.

information to an actual person or entity. The Supreme Court has applied this doctrine to statements made to undercover informants,[5] bank records released to banks,[6] and telephone numbers disclosed to phone providers.[7] The public disclosure doctrine, on the other hand, focuses on a suspect making voluntary public movements that are susceptible to visual surveillance. The Court has applied this doctrine to police surveillance of suspects using beeper technology[8] or a GPS device.[9]

Courts seem to pick and choose a doctrine when analyzing cell phone location data, with little to no analysis on why one or the other applies (or doesn't apply).[10] These inconsistent choices are primarily due to the unique nature of this technology and the different ways one can conceptualize how the government collects it. The data can be viewed as nonpublic information disclosed to a cell phone provider, suggesting a potential application of the third-party doctrine, or as public movements susceptible to visual surveillance, suggesting a potential application of the public disclosure doctrine. But the key to applying the right doctrine is recognizing in which of these two contexts the government activity is taking place. It matters, for example, whether the government is seeking historical cell phone location data or acquiring real-time data. This Essay provides the first workable topology for these various scenarios and, in the process, offers some much overdue clarification on the operative elements of the respective doctrines.

Part I introduces how cell phone location data is created and collected. Part II details the contours of the third-party and public disclosure doctrines. Part III highlights the split among federal courts regarding whether the Fourth Amendment protects against the collection of cell phone location data, particularly in light of the varying applications of the third-party and public disclosure doctrines. Part IV outlines an approach for determining which of the two doctrines should apply. Finally, the Essay concludes by noting the implications of the cell phone location data Fourth Amendment conundrum for future technological developments.

---

[5] Hoffa v. United States, 385 U.S. 293 (1966).

[6] United States v. Miller, 425 U.S. 435 (1976).

[7] Smith v. Maryland, 442 U.S. 735 (1979).

[8] United States v. Knotts, 460 U.S. 276 (1983).

[9] United States v. Jones, 132 S. Ct. 945 (2012).

[10] *See, e.g.*, *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 312–13, 317–18 (3d Cir. 2010); *infra* Part III.

I. A PRIMER ON CELL PHONE LOCATION DATA

Cell phones use radio waves to connect to their service providers to facilitate a host of functions, including making and receiving phone calls, sending and receiving text messages, and using the Internet.[11] Cell phone providers, in turn, maintain thousands of cell phone towers that receive these radio signals.[12] Cell phones emit these signals anytime they are turned on, after which the nearest cell phone tower acquires a signal.[13] This process is automatic, without any notice to the user, and a user does nothing to facilitate the transmission except turning on the phone.[14] The signal moves from tower to tower as a cell phone user changes location and the location of the nearest tower is transmitted to the provider.[15] Cell phone company privacy policies typically include language that a user's location is collected in the foregoing way.[16]

It is useful to recognize three different scenarios under which the government tracks movements through the acquisition of cell phone location data: (1) historical cell phone location data, (2) real-time cell phone location data, and (3) actively "pinging" a cell phone for location data.

Cell phone providers store location data as the normal part of their business of providing service.[17] Police, in turn, can request that cell phone providers hand over this location data for a suspect over a set period of time.[18] This information is classified as historical cell phone location data.

This data stands in contrast to real-time location data. Whereas the former focuses on past locations, real-time data provides locations as they

---

[11] *See, e.g.*, State v. Earls, 70 A.3d 630, 637 (N.J. 2013) (discussing the basics of how cell phone location data works).

[12] *Id.*

[13] *Id.*

[14] United States v. Graham, 796 F.3d 332, 354–55 (4th Cir. 2015); *Earls*, 70 A.3d at 637.

[15] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 702 (2011); *see also Earls*, 70 A.3d at 637 ("Network-based location tracking relies on the network of cell sites and antennas . . . ."). Depending on the provider and particular cell phone, the actual location of the cell phone may also be transmitted. Freiwald, *supra* at 713 (discussing how certain smart phones are equipped with GPS capability and that the phone's specific location may also be transmitted to a provider). Because this additional transmission may reveal otherwise private information, the Fourth Amendment analysis under the public disclosure doctrine could potentially come out differently. *See infra* note 40 and accompanying text.

[16] *Graham*, 796 F.3d at 345.

[17] *Earls*, 70 A.3d at 637.

[18] *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); *Graham*, 796 F.3d at 340–41, 343 (stating "[t]he precision of this location data depends on the size of the identified cell sites' geographical coverage ranges").

actually occur.[19] Here, cell phone providers, upon request, give police contemporaneous data on the location of the nearest cell tower for tracking purposes.[20]

Pinging a cell phone is a variation on the collection of contemporaneous cell phone location data. This time, however, the government does not wait for the phone itself to send its routine signal to the cell tower. Rather, the police request that cell phone providers send an affirmative signal to the suspect's phone to monitor her location via cell towers.[21]

II. FOURTH AMENDMENT DISCLOSURE DOCTRINES

A. The Contours of the Third-Party Doctrine

The basic premise of the third-party doctrine is readily known: an individual loses all reasonable expectation of privacy to information she discloses to another person or entity.[22] The roots of the doctrine trace back to the use of government informants. The government has always had the unfettered ability to elicit incriminating statements from unwary suspects.[23] As the Court has explained, it is of no consequence that a defendant revealed the information "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[24] This misplaced belief does not change the fact that the defendant voluntarily disclosed the information and thus took the risk that the government might obtain it without a warrant and use it against her at trial.[25] The Court has expanded the application of the doctrine to include

---

[19] *See* Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes?*, 8 FED. CTS. L. REV. 215, 217 (2015).

[20] *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 132–33 (E.D.N.Y. 2013). If available, police may also request the historical location data of the actual cell phone. Freiwald, *supra* note 15, at 713–14 (noting that certain police departments request the actual cell phone location whereas others only request the nearest cell tower).

[21] United States v. Caraballo, 963 F. Supp. 2d 341, 350–51, 360 (D. Vt. 2013). Users are not aware that this pinging is taking place. *Id.* at 350, 360.

[22] Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1820–26 (2014) (discussing evolution of third-party doctrine before and after *United States v. Katz*).

[23] *See* Hoffa v. United States, 385 U.S. 293, 302–03 (1966); Lopez v. United States, 373 U.S. 427, 437–39 (1963).

[24] United States v. Miller, 425 U.S. 435, 443 (1976); *see also Hoffa*, 385 U.S. at 302 ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

[25] *Miller*, 425 U.S. at 443. For this reason, some scholars talk about the principle as a waiver or consent principle. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561,

voluntary disclosures made to entities such as banks and telephone companies.[26]

A central feature of the doctrine is whether the disclosure was voluntary or otherwise not coerced. As one simple example, eliciting incriminating statements by putting a gun to a suspect's head would, in all likelihood, not satisfy the voluntariness requirement. This seems like an easy case. More recently, courts and scholars have questioned this requirement of voluntariness—and in turn, the application of the third-party doctrine—in today's technology-dominated world where we routinely (and almost necessarily) make many disclosures to many entities.[27] Whether it is disclosures to banks or e-mails sent via Internet service providers, we are constantly making disclosures to third parties. Should these actions appropriately be considered voluntary? There may not be an easy answer here.[28] Indeed, part of the disagreement on whether the third-party doctrine applies to cell phone location data stems from this issue of voluntariness.[29]

So ends the typical discussion of the doctrine. But this summary neglects some important considerations that bear on its application. The first relates to when the government can acquire the information. Is the government free to acquire the information at any point before it is conveyed to the third party, or must the information come from the third party itself?

Take the facts of *Smith v. Maryland*.[30] There, the government collected a dialed telephone number after it was conveyed to a telephone company in the normal course of making a call. But if the number is not protected due to its disclosure to the phone company, can the government acquire it before it reaches the company? On the one hand, the police could not, without first getting a warrant, enter a suspect's home and observe the suspect dial the number.[31] But what about tapping into public lines and acquiring the number before it reaches the company? This action would not

588–90 (2009); Sonia K. McNeil, Note, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 216–18 (2011).

[26] Smith v. Maryland, 442 U.S. 735, 745–46 (1979); *Miller*, 425 U.S. at 443.

[27] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (questioning the viability of the third-party doctrine in today's technology-dominated society); Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 25–28 (2013) (discussing scholars' reactions to technological advancements when it comes to the application of the third-party doctrine).

[28] Bedi, *supra* note 27, at 27.

[29] *See infra* Part III.

[30] 442 U.S. 735.

[31] *See* United States v. Karo, 468 U.S. 705, 717 (1984).

otherwise seem to implicate the suspect's individual Fourth Amendment rights.[32]

The analysis in *Smith* suggests that the government must retrieve information from and with the knowledge of the third party. Otherwise, the assumption of risk analysis loses its meaning. The whole point of the expectation that a government informant or telephone company might disclose information assumes in the first instance that they have received some information.[33]

It also seems that the disclosed information must be nonpublic. It is no accident that the Court talks about misplaced trust when discussing the effect of the doctrine.[34] The premise here is that the information is not public and that the person assumes the risk that the third party will nonetheless hand it over to the government. If the information were otherwise publicly available, the individual wouldn't really be taking on any additional risk by disclosing it to the third party. The above cases bear this out.[35] Whether it is statements to a confidential informant, bank statements to a bank, or telephone numbers to a phone company, each of these types of information are private or not otherwise publicly available.

B. The Contours of the Public Disclosure Doctrine

Courts and scholars alike often associate the public disclosure doctrine and third-party doctrine as expressing a singular principle.[36] In some ways, this makes sense, as both doctrines involve voluntary actions by suspects that, in turn, vitiate Fourth Amendment protection. With the public disclosure doctrine, however, the focus is not on disclosing information but rather on making public movements or those movements that are susceptible to visual observation. In short, a suspect does not have a reasonable expectation of privacy in her voluntarily disclosed public

---

[32] *See* Rakas v. Illinois, 439 U.S. 128, 133–34 (1978) (reaffirming that Fourth Amendment protection only applies where individual has a *personal* expectation of privacy).

[33] This doesn't mean that the government would need a warrant to tap into the public phone lines, but rather simply that the third-party doctrine would not seem to play a role here in assessing Fourth Amendment protection (or the lack of it).

[34] *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302–03 (1966).

[35] *See Smith*, 442 U.S. 735; United States v. Miller, 425 U.S. 435 (1976); *Hoffa*, 385 U.S. 293.

[36] *See* United States v. Jones, 132 S. Ct. 945, 956–57 (2012) (Sotomayor, J., concurring) (discussing the general viability of the third-party doctrine when assessing the permissibility of long-term GPS surveillance); United States v. Knotts, 460 U.S. 276, 283 (1983) (referencing *Smith v. Maryland* as the "factual counterpart" to beeper monitoring); Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in* United States v. Jones, 123 YALE L.J. F. 393 (2014); Bedi, *supra* note 22, at 1820–26; Kerr, *supra* note 25, at 588–90.

movements.[37] In *United States v. Knotts*, for example, the police surreptitiously placed a beeper in the defendant's belongings and used it to follow the defendant for a few hours to his ultimate destination.[38] The Court found no problem with this type of surveillance, reasoning that:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction . . . .[39]

The key here is that the police only monitored public movements, not movements within a person's home where the Fourth Amendment would clearly apply.[40] Moreover, it didn't matter that the suspect was unaware of the beeper transmission or that the police were not in constant visual contact with the car as long as the movements were susceptible to visual surveillance.[41] The analysis of *Knotts* under the third-party doctrine, on the other hand, would have come out differently. Since the suspect was not aware of the beeper and its emanating signal, the suspect could not have voluntarily disclosed his movements to the police.

The public disclosure doctrine thus does not implicate the same issues of *how* or *when* the government obtains information. The reason for this is the public nature of the movements (e.g., the car's location) serves as the sole trigger. Because this information is susceptible to visual observation, it is *per se* not protected under the Fourth Amendment.

One can still use the assumption of risk calculus with the public disclosure doctrine but it looks different than the third-party doctrine analysis. The risk here relates to the government's surveillance of a

---

[37] Bedi, *supra* note 22, at 1820–26 (discussing evolution of public disclosure doctrine before and after *United States v. Katz*).

[38] *Knotts*, 460 U.S. at 277.

[39] *Id.* at 281–82.

[40] *Compare Knotts*, 460 U.S. 276, *with* United States v. Karo, 468 U.S. 705, 714–15 (1984) (finding that monitoring movements within the home triggered Fourth Amendment protection). The concern over nonpublic information may potentially impact how one analyzes location data of an actual cell phone as opposed to a public cell tower under the Fourth Amendment. If the former location data reveals a person's movements in her home or a place where she has a reasonable expectation of privacy, the public disclosure doctrine would not apply. *See, e.g.*, *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 312–13 (3d Cir. 2010) (citing the *Knotts–Karo* distinction when discussing the potential of historical location data revealing nonpublic locations but concluding the distinction not relevant on instant facts because the government only acquired cell tower or public location data).

[41] *Knotts*, 460 U.S. at 285.

person's public movements rather than its acquisition of private information from an entity or person.[42]

The public disclosure doctrine is not without potential limits. *Knotts* itself suggested that a different conclusion may be necessary if the monitoring lasted a day or longer.[43] It is telling that the Court made explicit that "different constitutional principles" would be needed to analyze this long-term surveillance, and in doing so, cited to a First Amendment-related case.[44] This analysis implies that the public disclosure doctrine on its own would treat long-term surveillance no differently than short-term surveillance—neither would receive Fourth Amendment protection.

This concern over the potentially harsh implications of long-term electronic surveillance under the public disclosure doctrine leads to the most recent case on the doctrine, *United States v. Jones*.[45] Here, the government—without the consent of the defendant or under the terms of a warrant—installed a Global Positioning System (GPS) device under his car and tracked his public movements with the device for nearly thirty days.[46] The Court (both the majority and concurrences) wrestled with how this government activity could fall under the scrutiny of the Fourth Amendment when the public disclosure doctrine mandated that none of this surveillance would garner constitutional protection.[47] The majority focused on the initial act of placing the GPS device as constituting an unlawful physical trespass, whereas the concurrences focused on the revelation of private information (e.g., political affiliations) as a byproduct of long-term GPS surveillance.[48] Analysis of these limiting principles is beyond the scope of this Essay.[49]

---

[42] In turn, the debate over the voluntariness of disclosing location data under the third-party doctrine isn't an issue in the public disclosure context. The cell phone user quite obviously has voluntarily exposed her public movements to potential visual observation.

[43] The concern here was dragnet activity by the government. *Knotts*, 460 U.S. at 283–84.

[44] *Id.* The Court cited to *Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978), which found that the Fourth Amendment warrant requirement adequately protects First Amendment interests. *Knotts*, 460 U.S. at 283; *see also* Bedi, *supra* note 22, at 1848–57 (discussing First Amendment values in Fourth Amendment reasonable expectation analysis).

[45] 132 S. Ct. 945 (2012).

[46] *Id.* at 948.

[47] *Id.* at 951–52 (explaining that while there is no reasonable expectation of privacy in public movements, this did not overturn the common law trespass doctrine); *id.* at 956 (Sotomayor, J., concurring) ("I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques."); *id.* at 964 (Alito, J., concurring) (citing *Knotts* for the proposition that short-term surveillance does not trigger Fourth Amendment protection).

[48] *Id.* at 950–54 (majority opinion); *id.* at 955–57 (Sotomayor, J., concurring); *id.* at 961–64 (Alito, J., concurring). The theory put forth by the concurrences has been dubbed the "mosaic theory." *See* Bedi, *supra* note 22, at 1834–38.

[49] For a discussion on the physical trespass doctrine and the mosaic theory, see generally Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV.

What matters for my purposes is that the majority decision bypassed the chance to alter the contours of the public disclosure doctrine, which for now does not hinge on the length of surveillance.[50]

III. DISAGREEMENT AMONG FEDERAL COURTS ANALYZING FOURTH AMENDMENT PROTECTION FOR CELL PHONE LOCATION DATA

A. No Reasonable Expectation of Privacy

A number of federal circuits have found that cell phone location data does not garner Fourth Amendment protection. Both the Fifth and Eleventh Circuits, in their assessments of the collection of historical location data, relied on a straightforward application of the third-party doctrine and suspects making a voluntary disclosure.[51] The Fifth Circuit, for example, analogizing to *Smith v. Maryland*, reasoned, "A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call."[52]

The Third Circuit, in reaching a similar conclusion, focused instead on the public disclosure doctrine.[53] Citing *Knotts*, the court explained:

> We cannot reject the hypothesis that [historical cell phone location data] may, under certain circumstances, be used to approximate the past location of a person. . . . [Prior opinions] make clear that the privacy interests at issue are confined to the interior of the home. There is no evidence in this record that historical [cell phone location data] . . . extends to that realm. We therefore cannot accept the . . . conclusion that [this data] . . . requires probable cause for its production.[54]

The Third Circuit's point here seems to be that historical cell phone location data is no different from the location data documented by other

1283 (2014); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 1, 17–32 (2012).

[50] *Jones*, 132 S. Ct. at 954 (majority opinion) ("It may be that achieving [four-week surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."). In fact, drawing a defensible line as to when surveillance becomes *too* long to fall under the public disclosure doctrine seems untenable. *See* Bedi, *supra* note 22, at 1839–48 (discussing various problems with the mosaic theory).

[51] United States v. Davis, 785 F.3d 498 (11th Cir. 2015); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

[52] *In re* Application of the United States for Historical Cell Site Data, 724 F.3d at 613; *see also Davis*, 785 F.3d at 512.

[53] *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

[54] *Id.* at 312–13.

tracking device technology that simply catalogs public locations. Interestingly, however, and in contrast with the Fifth Circuit, the Third Circuit went on to explain that the third-party doctrine would not necessarily support the same conclusion because a cell phone user does not voluntarily share location data with her cell phone provider.[55]

Real-time location data would appear to stand or fall with historical location data. This information is also initially disclosed to a cell phone provider, albeit quickly transmitted to the government thereafter. For this reason, some courts have treated historical and real-time data the same way, finding no protection based on an application of the third-party doctrine.[56]

The Sixth Circuit has gone one step further by finding that pinging a cell phone user's phone to ascertain her real-time location also does not trigger Fourth Amendment protection.[57] In reaching its conclusion, the court distinguished between the effects of the public disclosure doctrine and the third-party doctrine in this context.[58] The court analogized to *Knotts* and reasoned that the police could have acquired "that same information . . . through visual surveillance."[59] However, in an earlier case, the court also seemed to recognize that the third-party doctrine may suggest a different outcome.[60] It was the government's act of pinging the cell phone that triggered the location, not a voluntary act by the cell phone user.[61] However, because the real-time data was simply a proxy for a suspect's public location, there was no Fourth Amendment protection.[62]

B. Finding Reasonable Expectation of Privacy

Other courts have found that this data should, at least in some circumstances, garner Fourth Amendment protection. These decisions often emphasize the voluntariness element (or lack of it) in the application of the

---

[55] *Id.* at 317.

[56] *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 145–47 (E.D.N.Y. 2013); United States v. Booker, No. 1:11-CR-255-1-TWT, 2013 WL 2903562, at *9 (N.D. Ga. June 13, 2013).

[57] The Sixth Circuit has ruled in two cases on this matter. United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); United States v. Forest, 355 F.3d 942 (6th Cir. 2004), *cert. granted, judgment vacated on other grounds sub nom.*, Garner v. United States, 543 U.S. 1100 (2005).

[58] *Forest*, 355 F.3d at 951–52.

[59] *Skinner*, 690 F.3 at 778. Similar to *Knotts*, the court found that it was not crucial that the government may not have had visual contact throughout the full-length surveillance. The key fact was that the movements *could* be observed by visual observation. *Id.* at 779.

[60] *Forest*, 355 F.3d at 951.

[61] *Id.*

[62] *Id.*

third-party doctrine. The most recent decision on the issue comes from the Fourth Circuit, which found that, unlike the telephone user in *Smith v. Maryland* who knowingly conveyed the number dialed, the cell phone user did not voluntarily share her location in any meaningful way.[63] The court reasoned, "A cell phone user cannot be said to 'voluntarily convey' to her service provider information that she never held but was instead generated by the service provider itself without the user's involvement."[64] The court also found that the fact that the company's privacy policy mentioned this collection did not suggest a different conclusion since most users are not familiar with or otherwise understand their providers' policies.[65]

The Third Circuit reached a similar conclusion on the issue of voluntariness.[66] But what makes its decision so interesting is that the court simultaneously acknowledged that the public disclosure doctrine would suggest that this same data is not protected.[67] This tension between the two disclosure doctrines underscores the different foundational triggers underlying each. More on this later.

Some courts have also used the voluntariness element to distinguish *Smith v. Maryland* from real-time location data.[68] As one district court explained, "Unlike dialed telephone numbers, cell site data is not 'voluntarily conveyed' by the user to the phone company. [Rather,] it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge."[69]

It is interesting how these cases appear to discount the public disclosure doctrine. To the extent it applies, the doctrine does not depend on whether a court classifies the transmission of the location data as voluntary. Nor does it matter how the government acquired the data. All that matters is that the movements are vulnerable to visual observation.

The Fourth Circuit discussed the public disclosure doctrine but concluded it did not ultimately apply to the facts at hand. The court seemed to make a two-fold argument. First, it denied the basic premise that historical location data reveals otherwise public information. "[U]nlike GPS monitoring of a vehicle, examination of historical [cell phone data]

---

[63] United States v. Graham, 796 F.3d 332, 354 (4th Cir. 2015).

[64] *Id.* at 356.

[65] *Id.* at 345 & n.3.

[66] *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010).

[67] *See supra* notes 53–55 and accompanying text.

[68] *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005).

[69] *Id.*

can permit the government to track a person's movements between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home."[70] The court cited to the risk of cell phone tower location data revealing private information such as outpatient medical treatment or regular church visits.[71]

It is not clear whether this line of reasoning is ultimately persuasive. The same objection can also apply to public car movements such as those in *Knotts*. Police can surveil a suspect's car entering a church parking lot or medical complex. These acts would also seemingly reveal personal information but none are currently protected because of the public disclosure doctrine. Both cell phone tower data and a car's movements through streets are public information and thus stand or fall together.[72]

The Fourth Circuit also relied on the *Jones* concurrences in finding that the sheer amount of data revealed (in this case, it was movements over 220 days) militated against a straightforward application of the public disclosure doctrine.[73] These discussions on the privacy implications of long-term surveillance—while interesting and worthy of consideration—are ultimately beyond the scope of this Essay because current precedent dictates that all public monitoring—regardless of length—carries no Fourth Amendment protection.[74]

IV. PICKING AND CHOOSING BETWEEN THE DOCTRINES: A ROAD TO HARMONY

As the previous Part illustrates, courts seem to be all over the map when it comes to analyzing cell phone location data under the Fourth Amendment and whether this data merits protection. This disagreement largely centers on which doctrine a court uses and how it uses that doctrine.

Take, for example, the application of the third-party doctrine. A major point of contention is whether a cell phone user actually *voluntarily* discloses her location when making or receiving calls. This seems like a legitimate issue on which reasonable people can disagree. Because a user's

---

[70] *Graham*, 796 F.3d at 348.

[71] *Id.* (citing United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010)).

[72] A different constitutional conclusion under the public disclosure doctrine could result if the location data revealed the cell phone location rather than the public tower location. *See supra* note 40. However, only cell phone tower locations were at issue in *United States v. Graham*, 796 F.3d at 343.

[73] *Id.* at 349–51; *see also In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 118–19 (E.D.N.Y. 2011) (considering the public disclosure doctrine when tracking occurs for 113 days). *But see* United States v. Wilson, No. 1:11-CR-53-TCB-ECS-3, 2013 WL 1129199, at *5–7 (N.D. Ga. Feb. 20, 2013) (finding no Fourth Amendment violations in a request limited to cell phone tower data over a twenty-one day period).

[74] *See supra* notes 43–50 and accompanying text.

location—unlike a dialed number—is automatically transmitted after the phone turns on, this action may not qualify as a voluntary disclosure. Scholars too disagree on this point.[75] Perhaps the question of voluntariness should influence how we analyze the doctrine in this context, particularly given how prevalent cell phone use has become.

The more troubling area of disagreement, however, and the focus of this Essay, is how we should pick between the third-party and public disclosure doctrines. The analysis is not as cut-and-dried, as evidenced by the different way courts have handled this choice. And the decision seems rather consequential when one considers that the public disclosure doctrine suggests none of this data is protected. To see the problem, one needs only to look at the Third Circuit and its explicit recognition that the two doctrines lead to different conclusions on the privacy question of historical location data.[76] Things get even more complicated when considering the other kinds of cell phone location data—real-time location data and pinged data—and the different ways courts have handled them. Are we simply left with ad hoc judgments on which doctrine to use in what context, or is there some principled way for courts to make this choice?[77]

The problem centers on the unique nature of cell phone location data. On the one hand, the government can treat it like the collection of nonpublic information, no different than dialed telephone numbers (think historical location data). On the other hand, this data can also be seen as publicly available data that facilitates surveillance, no different than GPS monitoring (think real-time location data).

Historically, the collection of nonpublic information and surveillance of public movements were neatly separated. Collection of bank records, telephone numbers, and incriminating statements are all information-gathering activities of nonpublic data that have nothing to do with surveillance of the suspect's physical location. On the other hand, use of

---

[75] *Compare* Freiwald, *supra* note 15, at 733–34 (finding voluntariness lacking), *with* Orin Kerr, *Fourth Amendment Stunner: Judge Rules that Cell-Site Data Protected by Fourth Amendment Warrant Requirement*, VOLOKH CONSPIRACY (Aug. 31, 2010, 2:46 AM), http://volokh.com/2010/08/31/fourth-amendment-stunner-judge-rules-that-cell-site-data-protected-by-fourth-amendment-warrant-requirement [http://perma.cc/X23K-PCJA] (finding sufficient voluntariness). *See also* Monu Bedi, *Texting the Government Your Location: The Case of Historical Cell Phone Location Data and Fourth Amendment Protection*, CASETEXT (Aug. 26, 2015), https://casetext.com/posts/texting-the-government-your-location [http://perma.cc/Q6UR-JPNR] (discussing the issue of whether users voluntarily disclose their location data).

[76] *See supra* notes 53–55, 66 and accompanying text.

[77] Scholarship on the subject is not much help here because those discussions are more general in nature. *See, e.g.*, Freiwald, *supra* note 15, at 733; Recent Case, State v. Earls, *70 A.3d 630 (N.J. 2013)*, 127 HARV. L. REV. 2164 (2014).

beeper technology and GPS are surveillance methods of a suspect's public movements that do nothing more than relay her physical location.[78]

Police use of cell phone location data has blurred the line between these two types of activities. The first step to harmonizing the doctrines, then, is ascertaining in which context the government activity occurs with the recognition that the application of two doctrines is not mutually exclusive. I take the three scenarios in turn.

A. Historical Location Data

The government seeking historical location data from the cell provider stands on the same footing as the government acquiring a history of telephone numbers from the telephone company over a period of time. Both scenarios only potentially trigger an application of the third-party doctrine. The government is collecting nonpublic information from a third party. Whether the doctrine actually applies of course still depends on whether the disclosure of data to the provider is considered a voluntary one.

One may take issue with my conclusion that the public disclosure doctrine is inapplicable here. Were these movements not public at one time, thus triggering this doctrine? To be sure, the Third and Fourth Circuits discussed this doctrine at length in the context of historical location data, albeit reaching different conclusions as to its applicability.[79] But the problem here is we're talking about public data in the past tense. These *were* public movements and *at that time* the government could have surveilled the person's location using this data without first seeking a warrant. But these data points—at the point the government is now seeking them from the provider—are no longer public (i.e., susceptible to visual surveillance) and, as such, the risk of the government observing them has now passed, along with the application of the public disclosure doctrine. In fact, it seems odd to say that the government, in collecting *historical* data, is nonetheless surveilling the suspect's public movements when those movements are no longer taking place. This is not to say that the police cannot gather this historical data to conduct prospective surveillance of the suspect, but the suspect's potential *future* public movements are conceptually different from prior public movements and the collection of her historical location data. The latter are now no different than any other

[78] I recognize that location data (whether by GPS, beeper, or cell phone use) is also a type of information, and so even in the second scenario, the government is technically "collecting information." But the key difference here is that this information (unlike telephone data) is susceptible to visual observation and facilitates surveillance of the suspect.

[79] *See supra* notes 53–54, 70–73 and accompany text.

nonpublic information—whether it is telephone numbers, bank statements, etc.—the government acquires from a third party.[80]

In some ways, this is a better outcome for those who think historical location data deserves constitutional protection. If the public disclosure doctrine does not reach this data, there is no need to argue against its application. This conclusion renders moot much of the aforementioned Fourth Circuit discussion on the more private nature of cell phone versus automobile location data, as well as the concern over large amounts of surveillance records.

That said, the privacy implications of the latter could also work as a limiting principle for the third-party doctrine. While the operative facts of *Jones* dealt with contemporaneous surveillance, a historical map of an individual's movements over a lengthy period of time may also trigger privacy concerns for the same reason (e.g., revelation of a person's political affiliation or medical treatment).[81] Whether the effects of long-term historical data collection should be part of the third-party doctrine analysis is, again, beyond the scope of this Essay.

B. Real-Time Location Data

Categorizing real-time location data is a bit trickier. This kind of data can potentially be analyzed under both doctrines. In one sense, the government is acquiring information from the cell phone provider, very similar to historical data or telephone numbers. Whether the third-party doctrine is triggered, however, depends in large part on how one conceptualizes the risk of exposure. Certainly, as previously explained, the main thrust of the doctrine contemplates nonpublic information. Still, one could argue that this doctrine does not require only *one* risk. In other words, an individual could be taking on both the risk that the user's location may be disclosed by the particular third party as well as the risk that it is currently susceptible to public view.[82]

---

[80] A potential—though ultimately unpersuasive—counterargument would be that under the public disclosure doctrine, once something has been made public, it is public for good. This line of reasoning would conclude that historical location data—because it was at one point public—is forever considered public information. This is a strained reading of the doctrine as the Court has applied it. These cases and their operative facts, *see supra* Section II.B, clearly contemplate contemporaneous visual observation. To hold otherwise would make meaningless the surveillance activity being conducted by the police in all these cases. Moreover, this line of reasoning would also mean that once information is made public, albeit even briefly, it could never garner Fourth Amendment protection. This seems like a drastic conclusion that would have severe, unwanted implications for privacy protection.

[81] *See supra* notes 45–50, 73 and accompanying text.

[82] Of course, there remains the question of whether the disclosure to the cell phone provider is voluntary.

This is an interesting discussion but ultimately turns out to be irrelevant when assessing Fourth Amendment protection. Whichever way one answers the question of the *potential* reach of the third-party doctrine to real-time location data, there is no privacy protection because the public disclosure doctrine obviously applies. The government is using public location data—i.e., movements susceptible to visual surveillance—to contemporaneously track a suspect.[83] This is no different than the government using a beeper or GPS device to surveil an individual.

While the applicability of the public disclosure doctrine is straightforward, the operative facts for the third-party doctrine may not be present. This is not problematic. These doctrines were never designed to both be necessary conditions for vitiating privacy protection. Take the *Knotts* case. There, *a fortiori*, the third-party doctrine does not apply because the suspect—lacking knowledge of the beeper—could not possibly have voluntarily conveyed his location to the government. This fact was not relevant to the lack of privacy protection because the suspect's public movements fell directly under the public disclosure doctrine.

The difference in Fourth Amendment protection between real-time data (*automatically not* protected under public disclosure doctrine) and historical data (*may not* be protected under the third-party doctrine) makes sense when assessing the relative privacy concerns in each scenario. With stored data, the police can have easy access to significant amounts of location history. There is no practical limitation to the timeframe they may acquire. This concern may militate in favor of having a robust requirement of voluntariness under the third-party doctrine so it is harder to acquire this information without Fourth Amendment protection. On the other hand, use of real-time data has some built-in practical limitations. It requires at least some sort contemporaneous police surveillance (even if alleviated by the relevant technology), which naturally limits how much data is collected. Here then, a straightforward application of the public disclosure doctrine may not be as detrimental to privacy concerns.

C. Location Data from Pinging

Analysis of the third scenario involving pinging a cell phone would work in a similar way to real-time data. Here, the third-party doctrine is clearly not applicable because there has been no disclosure by the cell phone user. It is the cell phone company—in concert with the government—that is actively sending signals to the cell phone. Once again, though, the public disclosure doctrine squarely applies because the

[83] I assume here that the location data only reveals public locations such as the cell tower location.

government is tracking the public movements of the cell phone user via the provider's cell towers.[84] Those who feel that real-time location data should garner Fourth Amendment protection must argue for the Court to adopt some limiting principle—e.g., length of surveillance—to curtail the impact of the public disclosure doctrine.

CONCLUSION

The lessons here go beyond cell phone location data. If there is anything to be certain of, it is that technology will continue to advance. This inevitably will lead police to having better information-gathering capacity and surveillance ability. Unless the Court acts, the third-party and public disclosure doctrines will continue to stand as two central hurdles to Fourth Amendment protection in these situations. It is important we understand the historical context and unique contours of each doctrine. Only then can we intelligently discuss whether and how they should, or should not, apply to future technologies.

[84] This conclusion, again, assumes that the government is only receiving the cell phone tower location and not the actual location of the cell phone. Acquiring the latter through pinging the phone may sweep in nonpublic information and thus change the analysis. *See supra* note 40. A similar conclusion would potentially apply to "stingray" devices, assuming that they also only reveal public locations. These devices mimic cell phone towers and have the ability to gather location data without permission of the cell phone provider and before it reaches the cell tower. *See, e.g.*, Brian L. Owsley, *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, 113 MICH. L. REV. FIRST IMPRESSIONS 75, 76 (2015). While scholars and courts seem to find that these devices constitute a search under the Fourth Amendment, *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012); Owsley, *supra*; Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 32 (2014), a straightforward application of the public disclosure doctrine would suggest otherwise because these movements would be susceptible to visual observation.